Claims 1 – 28 have been examined and stand rejected under 35 U.S.C. §103(a). The rejections are respectfully traversed and the following remarks are intended to place the application in better form for consideration on appeal. For the Examiner's convenience, a copy of the pending claims is set forth in an Appendix.

The pending claims are directed to a method and system for providing financial services over a public network. As explained in the specification, this is performed in an embodiment by using a portable computer-readable storage medium as a substitute for a more traditional debit card (Application, p. 4, ll. 24 – 26). As a counterpart to a traditional debit card, this computer-readable storage medium includes information similar to that contained on the magnetic stripe of a debit card. Notably, however, this information is encrypted on the computer-readable storage medium, while a traditional debit card does not include any encrypted information. The computer-readable storage medium may be used for electronic commercial transactions in a manner similar to how a debit card is used: when a customer wishes to purchase a product from a Web site, a microprocessor in the customer's personal computer retrieves the encrypted information from the computer-readable storage medium and transmits it to a server, which then forwards a request to debit a specified amount with the encrypted information (*id.*, p. 5, ll. 5 – 17). These features are reflected in independent Claims 1, 17, and 26 with language that requires *encrypted information retrieved from a computer-readable storage medium to be used in determining access to a customer's financial account.*

This is neither taught nor suggested in the references cited in the rejections of the independent claims. In particular, those rejections cite a combination of U.S. Pat. No. 5,903,881 ("Schrader") and U.S. Pat. No. 5,457,746 ("Dolphin").

Schrader is cited for its disclosure of on online banking system (Second Office Action, p. 4) and it is noted that that the computer application may be delivered to the user on a CD ROM (*id.*, p. 5). The use of a CD ROM in this context, however, is

nothing more than as a delivery means for the software product, with Schrader noting that other delivery means could also be used (Schrader, Col. 12, ll. 62 – 67). Notably, the CD ROM is *not* needed to perform any of the banking applications described in Schrader after the computer program has been installed on a user's computer. In this respect, it is no different than most commercially available software. The Office Action also notes that Schrader discloses an encryption module for exchanging transaction information (Second Office Action, p. 2). This is not believed to be relevant to the claims because they never recite performing an encryption as disclosed by Schrader; they instead recite the very different function of retrieving *previously encrypted* information from the computer-readable storage medium. In addition, Schrader only discloses encrypting transaction information; it specifically draws a distinction between the different security features of "user authentication" functions and encryption of transaction information (*see, e.g.,* Schrader, Col. 17, ll. 12 – 15).

The Office Action concedes that Schrader does not disclose retrieving encrypted information from the computer-readable storage medium (*id.,* p. 6), and cites Dolphin for this disclosure (*id.,* p. 2). Dolphin is directed to controlling access to publications of periodicals — multiple periodicals are encrypted onto a CD ROM and a customer is given access only to those he has paid for by providing the corresponding access codes (Dolphin, Col. 2, ll. 34 – 44). Dolphin never discloses doing anything with encrypted information other than decrypting it for the user to read. It certainly does not disclose using it to determine access to a customer's financial account as all the independent claims require.

Thus, in part, a *prima facie* case of obviousness has not been established since no motivation to combine the references has been shown. The Office Action seems to suggest that the level of skill in the art is relied upon for such a motivation (Second Office Action, p. 3), but such a basis is improper (*see* MPEP 2143.01, "The level of skill in the art cannot be relied upon to provide the suggestion to combine references").

A *prima facie* case of obviousness has also not been established because none of the prior art cited discloses the claim limitation of decrypting retrieved encrypted information such that a financial institution determines an access to a customer's financial account (*see* MPEP 2143.03). Since such a limitation is included in all of the independent claims, all of the pending claims are patentable over the cited art. While it is believed that combining Schrader and Dolphin is improper, the omission of this element is especially highlighted by assuming *arguendo* that they may be combined. In particular, Schrader teaches providing unencrypted online banking software on a CD ROM and Dolphin teaches providing multiple encrypted products on a CD ROM to restrict access to particular ones. At best, the combination of Schrader and Dolphin would therefore teach providing multiple encrypted software products on a CD ROM, one of which is online banking software, and providing access keys to particular software products based on which ones a purchaser has paid for. Nothing in Schrader, Dolphin, or their combination teaches or suggests using information encrypted on the CD ROM in the manner required by the claims.

Since all of the independent claims are patentable over the cited art, all of the claims that depend from them are also patentable over the cited art.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,

Patrick M. Boucher
Reg. No. 44,037

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: (303) 571-4000
Fax: (303) 571-4321
PMB
DE 7076097 v1

APPENDIX: PENDING CLAIMS

The complete set of currently pending claims is set forth below. No amendments have been made as part of the foregoing response.

1.   (As filed) A system for providing financial services over a public network accessible by a plurality of customers via respective network access devices with modems and over a private network accessible by a plurality of financial institutions via computers with modems, said financial institutions maintaining respective financial accounts for said plurality of customers, said system comprising:

a network access device including a programmable controller for executing code and a memory for storing a browser software to interface with said public network, a customer using said network access device and a computer-readable portable storage medium to access a customer's financial account via said public network, said computer-readable portable storage medium having encrypted and unencrypted information recorded thereon pertaining to said customer's financial account; and

a decryption processor, connected to said network access device via said public network, for decrypting said encrypted information retrieved from said storage medium such that a financial institution, connected to said decryption processor via said private network, determines an access to said customer's financial account on the basis of the decrypted information.

2.   (As filed) The system according to Claim 1, further comprising a computer connected to said network access device via said public network, said computer hosting a site for goods or services available on-line, said computer comprising a microprocessor being operative to transfer an active module to said network access device in response to said customer requesting the access to said customer's financial account by using said computer-readable portable storage medium.

3.   (Once Amended) The system according to Claim 2, wherein said active module contains code which is executed by said programmable controller in said network access device such that at least part of said unencrypted information is provided to said customer who is requested to enter a first identifier related to said customer's financial account.

4.   (As filed) The system according to Claim 3, wherein said programmable controller is operative to transfer the entered first identifier and the encrypted information to said computer for forwarding to said decryption processor.

5.   (As filed) The system according to Claim 4, wherein said decryption processor is operative to extract a second identifier pertaining to said customer's financial account from the decrypted information and to re-encrypt the extracted second identifier.

6.   (As filed) The system according to Claim 5, further comprising a network switch located on said private network for routing the re-encrypted second identifier received from said decryption processor to said financial institution maintaining said customer's financial account for determining whether to approve the access to said customer's financial account.

7.   (As filed) The system according to Claim 6, wherein said financial institution generates a code for indicating whether or not the access to said customer's financial account has been approved and transfers the generated code to said decryption processor via said network switch.

8.   (As filed) The system according to Claim 7, wherein customer's address data is displayed to said customer on said network access device if said code represents an access approval.

9.   (Once Amended) The system according to Claim 3, wherein the provided unencrypted information includes a name of said financial institution maintaining said customer's financial account.

10.   (Once Amended) The system according to Claim 3, wherein the provided unencrypted information includes an audio message pertaining to said financial institution maintaining said customer's financial account.

11.   (Once Amended) The system according to Claim 3, wherein the provided unencrypted information includes advertising information pertaining to said financial institution maintaining said customer's financial account.

12.   (As filed) The system according to Claim 1, wherein said computer-readable portable storage medium is a CD-ROM.

13.   (As filed) The system according to Claim 12, wherein said CD-ROM is produced by a card production facility, based on a card production file, for mailing said CD-ROM to said customer.

14.   (As filed) The system according to Claim 13, wherein said card production file includes an encrypted first identifier pertaining to said customer's financial account and said unencrypted information pertaining to said financial institution.

15. (As filed) The system according to Claim 14, wherein said encrypted first identifier is generated by an encryption module for encrypting a first identifier.

16. (As filed) The system according to Claim 15, wherein said first identifier prior to the encryption is generated by a card issuance system which is further operative to generate a second identifier pertaining to said customer's financial account, the generated second identifier being transferred to a mailer production facility for mailing to said customer.

17. (As filed) A method for providing financial services over a public network accessible by a plurality of customers via respective network access devices with modems and over a private network accessible by a plurality of financial institutions via computers with modems, said financial institutions maintaining respective financial accounts for said plurality of customers, said method comprising:

accessing a customer's financial account via said public network using a network access device and a computer-readable portable storage medium having encrypted and unencrypted information recorded thereon pertaining to said customer's financial account;

retrieving said encrypted and unencrypted information from said storage medium; and decrypting the retrieved encrypted information such that a financial institution determines an access to said customer's financial account on the basis of the decrypted information.

18. (As filed) The method according to Claim 17, further comprising using said computer-readable portable storage medium in said network access device in response to an active module being downloaded to and executed at said network access device such that said unencrypted information is displayed to said customer.

19.   (As filed) The method according to Claim 18, further comprising entering an identifier pertaining to said customer's financial account in response to the executed active module.

20.   (As filed) The method according to Claim 19, wherein said unencrypted information includes a name of said financial institution maintaining said customer's financial account.

21.   (As filed) The method according to Claim 19, wherein said unencrypted information includes an audio message pertaining to said financial institution maintaining said customer's financial account.

22.   (As filed) The method according to Claim 19, wherein said unencrypted information includes advertising information pertaining to said financial institution maintaining said customer's financial account.

23.   (As filed) The method according to Claim 17, wherein said computer-readable portable storage medium is a CD-ROM.

24.   (As filed) The method according to Claim 23, wherein said CD-ROM is produced on the basis of a card production file that includes an encrypted identifier pertaining to said customer's financial account and said unencrypted information pertaining to said financial institution.

25.   (As filed) The method according to Claim 17, further comprising reviewing customer's address data displayed on a monitor of said network access device if said financial institution has approved the access to said customer's financial account.

26.   (As filed) A computer-readable portable storage medium having recorded thereon code, executable by a programmable controller, for providing financial services over a public network accessible by a plurality of customers via respective network access devices with modems and over a private network accessible by a plurality of financial institutions via computers with modems, said financial institutions maintaining respective financial accounts for said plurality of customers, said storage medium comprising:

first code means for storing encrypted information for accessing a customer's financial account via said public network; and

second code means for storing unencrypted information for displaying a name of a financial institution maintaining said customer's financial account in response to a customer using said storage medium in a network access device to request an access to said financial account.

27.   (As filed) The storage medium according to Claim 26, wherein said unencrypted information further includes an audio message pertaining to said financial institution.

28.   (As filed) The storage medium according to Claim 26, wherein said unencrypted information includes advertising information pertaining to said financial institution.